UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA	)	
	)	
VS.	)	CRIMINAL NO. SA-07-CR-253-XR
	)	
(01) DAVID WINKLER	)	

ORDER

Background

1. Beginning in October 2005, the United States Attorney's Office for the District of New Jersey and United States Immigration and Customs Enforcement ("ICE") officials investigated an illegal child pornography ("CP") website.

2. ICE learned of the basic structure and procedure for gaining access to this illegal CP website, which involved the submission of a credit card number that is then authenticated, and if accepted, the subscriber's email address was sent a link and password to the CP website. The charges for access to the CP website are then reflected on the cardholder's subsequent billing statement under a fictitious corporate name, which was later determined to be named "AdSoft."

3. In mid-December 2005, ICE agents, having discerned the CP website was hosted on a server in Florida, executed a search warrant which led to the discovery of CP and log files that contained the internet protocol[1] addresses of subscribers to the CP website.

[1] According to the ICE agent's affidavits, an internet protocol (I.P.) address is analogous to a telephone number in that "[e]very computer or device on the Internet is referenced by a unique Internet Protocol address. . . . An IP address is a series of four numbers separated by a period. . . . Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address." Docket No. 33, Exh. A at ¶9(e); Exh. B at ¶8(e).

4. On December 23, 2005, a search warrant was issued authorizing ICE to intercept electronic communications from the email address ("Dykstra Email Address") which disseminates the links and passwords for the CP websites.

5. On February 1, 2006, ICE, having learned that the CP website was now being hosted on a new server in Virginia, executed a search warrant, discovering CP and log files. These log files contained information about those who accessed the CP website. This information included the member's identification and login number, the member's email address, the start and end date of the member's subscription, as well as the member's I.P. address, a log of what content each member had accessed, and the time each member accessed said content.

6. From the results of the searches of the servers in Florida and Virginia, and the electronic surveillance of the Dykstra Email Address, ICE was able to identify hundreds of subscribers who had accessed the site between November 2005 and February 25, 2006. This investigation led to over two hundred search warrants and more than one hundred and fifty arrests.

7. Records obtained by ICE's September 2006 search of an online credit card purchase collection company ("JetPay") indicate a person, alleged to be the Defendant, on March 10, 2006, subscribed to the CP website using a MasterCard ending with the four digits 7171. The records further reflected this subscriber's address was [address redacted for privacy reasons], Kerrville, Texas. Also, the JetPay records included the password issued by the Dykstra Email Address, and the purchase price, which was identical to the charges reflected by the AdSoft entries found in the JetPay records, and later corroborated with MasterCard billing records.

8. On or about March 14, 2006, ICE was able to determine that the information supplied by subscribers to the CP website was sent through a certain server in California.

9. On May 4, 2006, ICE executed a search warrant on the California server and retrieved information regarding the date and time individuals subscribed to the CP website, as well as the subscriber's email and physical addresses. ICE agents corroborated this information to determine the email address of those who subscribed to the CP website between February and May 2006.

10. Records obtained by ICE's September 2006 search of JetPay indicate a person, alleged to be the Defendant, on May 6, 2006, subscribed to the CP website using a MasterCard ending with the four digits 7171. The records further reflected this subscriber's address was [address redacted for privacy reasons], Kerrville, Texas. Also, the JetPay records included the password issued by the Dykstra Email Address, and the purchase price, which was identical to the charges reflected by the AdSoft entries found in the JetPay records, and later corroborated with MasterCard billing records.

11. Next, ICE shifted its focus to the financial side of the CP website, and discovered several entities involved in the laundering and channeling of funds for the CP website. Particularly, ICE focused on the entities responsible for collection of on-line credit card payments, namely JetPay, and noticed the fictitious name associated with the CP website charges on subscribers' credit card billing statements, AdSoft, was a customer of the entities being investigated. Due to this investigation, ICE, on September 19, 2006, obtained a search warrant and discovered the records of credit card purchases billed by AdSoft between February 1, 2006 and mid-July 2006.

12. Eventually, ICE agents compared the information obtained from its investigations of the servers, the Dykstra Email Address, JetPay, and AdSoft, and found Defendant's name and information reflecting a purchase from AdSoft, which was at this time believed to be a cover for the illegal CP website. In addition, from June 2006 through January 2007, ICE officials compared and reviewed all of the information obtained from its various search warrants, and realized that an individual using an email address of dcwink@ktc.com attempted to subscribe to the CP website, and a physical address of [address redacted for privacy reasons], Kerrville, Texas. ICE recognized that the same address was found in the JetPay records for a March 10, 2006 purchase by a customer named "Winkler."

13. On March 1, 2007, ICE subpoenaed Defendant's MasterCard records for his card number ending in 7171, and received them on April 3, 2007. The credit card number is identical to the number found in the JetPay records, and the MasterCard records reflected charges by AdSoft for $79.99 on both March 10, 2006 and May 6, 2006.

14. On March 26, 2007, Defendant's internet service provider ("ISP") confirmed that the email address dcwink@ktc.com belonged to Defendant and that internet service was provided to Defendant at [address redacted for privacy reasons], Kerrville, Texas. Additionally, Defendant's ISP confirmed internet service began July 5, 2002, and was active on the dates Defendant's credit card was charged on March 10 and May 6, 2006 for the CP website subscriptions.

15. On an undetermined date, ICE agents queried the Texas Department of Public Safety discovering Defendant's date of birth, Texas Driver's License number, and residential address of [address redacted for privacy reasons], Kerrville, Texas.

16. Also, on an undetermined date, ICE agents learned of Defendant's occupation as a physician and obtained an address for his medical practice as [address redacted for privacy reasons], Kerrville, Texas.

17. On April 6, 2007, ICE agents conducted surveillance at Defendant's residential address and office location and confirmed Defendant resided at [address redacted for privacy reasons], Kerrville, Texas, and had an office at a Medical Plaza located at [address redacted for privacy reasons], Kerrville, Texas. Additionally, ICE agents observed Defendant driving a vehicle that was registered to Defendant at his residential address.

18. On April 17, 2007, a United States Magistrate Judge issued a search warrant for Winkler's residence. This warrant authorized a search of this residence and the seizure of a litany of items in connection with the advertisement, trafficking, receipt, distribution, and/or possession of CP.

19. On either April 18 or 19, 2007,[2] the search warrant for the residence was executed. This search initially revealed no evidence of CP; however, during the course of the search, Defendant disclosed to ICE agents that he had a personal computer at his medical office that was connected to the Internet utilizing the same ISP and email address as his residential computer. Additionally, Defendant's wife informed ICE agents that Defendant regularly spent 18 to 20 hours a day at his medical office.

20. Based upon the information obtained during the residential search, ICE agents, on April 19,

[2] There appears to be a conflict in the date of execution of the search warrant for Defendant's residence. Page 1 of the United States Government's Response to Motion to Suppress Evidence (Docket No. 33) states this search warrant was "issued April 17, 2007 and executed April 19, 2007. However, ¶49 to Exhibit B, which is the search warrant for Defendant's medical office, indicates the residential search warrant was executed April 18, 2007.

2007, obtained a second search warrant authorizing the search of Defendant's medical office. The terms of this search warrant are substantially identical to the terms found in the residential search warrant, and authorize the seizure of the same items.[3]

21. On April 19, 2007, ICE agents executed the medical office search warrant, and seized a computer located on the premises.

22. On May 2, 2007, an indictment was issued by the grand jury charging Defendant with possession of child pornography.

Analysis

Legal Standard

The United States Constitution provides that "no Warrants shall issue, but upon probable cause."[4] Despite having no clear definition, probable cause exists "where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found."[5] The issuing Magistrate's task is

> simply to make a practical, common-sense decision whether, given all of the circumstances set forth in the affidavit, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a

---

[3] The affidavit in support of the second search warrant differs from the residential search warrant in that it notes the initial forensic investigations of computers found at Defendant's residence revealed no evidence of child pornography. Additionally, the affidavit further states that during the residential search Defendant's wife informed ICE agents Defendant regularly spent 18 to 20 hours a day at his medical office; Defendant informed ICE agents that he has a computer in his medical office, and that this computer is connected to the internet utilizing the same internet service provider and email address as his residential computers; and Defendant refused to grant his consent for a search of the computer at the medical office. *See* Docket No. 33, Exh. B at ¶¶49 - 52.

[4] U.S. CONST. amend. IV.

[5] *Ornelas v. United States*, 517 U.S.690, 696 (1996) (citing *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *Brinegar v. United States*, 338 U.S. 160, 175-76 (1949)).

> reviewing court is simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing]' that probable cause existed.[6]

The absence of clear rules for evaluation of probable cause has been aptly explained by the United States Supreme Court when it stated "[p]robable cause is a fluid concept-turning on the assessment of probabilities in particular factual contexts-not readily, or even usefully, reduced to a neat set of legal rules."[7]

As further guidance, the Fifth Circuit has provided that probable cause must be found within a sworn, written affidavit, and "does not require proof beyond a reasonable doubt; a magistrate need only have a substantial basis for concluding that a search would uncover evidence of wrongdoing."[8] Additionally, the "magistrate's determination is entitled to deference by reviewing courts."[9]

The Parties' Contentions

Defendant, in his Motion to Suppress Evidence (Docket No. 29), argues the search warrants issued for the search of his residence and his office lacked probable cause, and, alternatively, the ICE agents did not execute the search warrants based on a good faith belief in their validity.

Defendant bases his argument that the search warrants lacked probable cause on the assertion that the information relied upon was stale. Defendant initially argued that the information ICE agents relied upon was obtained in March 2006, making the information some thirteen months old when ICE obtained the warrant in April 2007. In his Post Hearing Memorandum (Docket No. 43),

---

[6] *Gates*, 462 U.S. at 238-39 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

[7] *Id.* at 232.

[8] *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (citing *United States v. Brown*, 941 F.2d 1300, 1302 (5th Cir. 1991)).

[9] *Id.* See also, *United States v. Ventresca*, 380 U.S. 102, 109 (1965).

Defendant urges a similar argument. However, Defendant argues the determinative date for staleness purposes was the search of the server in Alta Vista, California, in May 2006; thus making the information relied upon ten months old. Additionally, Defendant asserts, without legal authority, that there must be evidence of actual access to the child pornography website, not just evidence of a subscription.

In support of his staleness argument, Defendant cites a Seventh Circuit case which found insufficient probable cause to support a search warrant in a child pornography case.[10] The *Doan* Court concluded "a warrant with seventeen-month-old information" does not "per se lack probable cause."[11] However, the Seventh Circuit did state that "the older the information is regarding child pornography, the more necessary it is to include more detail concerning the person who is the subject of the investigation."[12] Defendant argues ICE agents failed to include the requisite specific information necessary to overcome the alleged staleness issues of the information concerning CP access and subscription relied upon in the ICE affidavit.

Citing another Seventh Circuit case, the *Doan* Court recognized that the age of the information found in an affidavit is merely one of the factors considered.[13] Besides age of the information, consideration of the "'[c]redibility of informants, [and] nexus to the searched premises and to illegal activity'" are relevant to a probable cause inquiry, but that "'no single piece of

---

[10] See *United States v. Doan*, 2007 WL 2247657 (7th Cir. Aug. 6, 2007) (finding information used to support affiant's assertion was stale as it was in excess of seventeen months old; therefore, that information was insufficient to support probable cause for issuance of a search warrant).

[11] *Id.* at *4.

[12] *Id.*

[13] *Id.* at *3 (quoting *United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007).

information need satisfy every relevant consideration before [the court] may consider it.'"[14] It appears the *Doan* Court made its decision on a lack of other evidence verifying the defendant was violating child pornography laws, and pointed out the only information connecting the defendant to child pornography was the seventeen month old paid website subscriptions.[15] Additionally, the *Doan* affiant's conclusory notation that he had experience with child pornography information in excess of eighteen months' age failed to cure the staleness issue.[16]

Additionally, Defendant claims that ICE, at the time the search warrant was issued, had no evidence that (1) Defendant "either logged onto a child pornography website or that he downloaded any child pornography onto his computer;"(2) Defendant either owned or possessed a computer; and (3) the Alta Vista server contained an IP address belonging to Defendant.[17]

The United States opposes Defendant's motion by arguing evidence of actual possession of child pornography is unnecessary for probable cause, the information relied upon to support probable cause was not stale, and, alternatively, ICE agents exercised good faith in its objectively reasonable reliance upon the magistrate's finding of probable cause when they executed the search warrants.[18]

Specifically, the United States cites a Fifth Circuit case for the proposition that an affidavit in support of a search warrant for child pornography need not "contain specific, individualized

---

[14] *Id.* (quoting *United States v. Wiley*, 475 F.3d 908, 915 (7th Cir. 2007).

[15] *Id.*

[16] *Id.*

[17] Docket No. 43 at 4-5.

[18] See generally, Docket No. 33.

information that a defendant possesses child pornography."[19] The *Flanders* case is premised upon language found in *Froman* that points out some unique circumstances of a child pornography case.[20] Particularly, the *Froman* court noted "that it is common sense that a person who voluntarily joins [a child pornography website], remains a member of [the website] for approximately a month without cancelling his subscription, . . . would download such pornography from the website and have it in his possession."[21]

Next, the United States argues the information the affiant relied upon is sufficient to support probable cause regardless of its age because of other specific information provided in support of the affidavit. Particularly, the United States cites evidence that (1) the affiant's knowledge, experience, and training provides the basis for the belief that computers are used extensively in the production, communication, distribution, and storage of child pornography;[22] (2) the affiant's knowledge, experience, and training provides the basis for the belief that subscribers to child pornography websites are usually collectors of such material, and that collectors of child pornography frequently hoard their collection and store such material on computers for long periods of time;[23] and (3) other information regarding prior multiple subscriptions to child pornography websites created a belief that

---

[19] *United States v. Flanders*, 468 F.3d 269, 271 n3 (5th Cir. 2006) (citing *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004)).

[20] *Id.*

[21] *Froman*, 355 F.3d at 890-91.

[22] Docket No. 33, Exh. A at ¶¶11(a) - (d), 12; Exh. B at ¶¶10(a) - (d), 11.

[23] Docket No. 33, Exh. A at ¶47(a) - (f); Exh. B at ¶46(a) - (f).

Defendant was a collector of child pornography.[24]

Analysis of the Arguments

Generally, courts undertake a two-part review of a motion to suppress evidence.[25] The first inquiry is "whether the good-faith exception to the exclusionary rule applies."[26] If the exception applies, there is no need to undergo the second part of the analysis, which is a determination of "whether the magistrate had a substantial basis for finding probable cause."[27] However, this Court will address the probable cause issue first.

Probable Cause

The Court must determine whether there was probable cause sufficient to issue a search warrant. Addressing Defendant's staleness argument, the instant case is easily distinguishable from the *Doan* case in that the ICE agents compiled detailed information, set out above, from several sources that was corroborated to conclude Defendant had subscribed to a website displaying child pornography. Although there can be no bright-line test for staleness, the information used in the instant case was, by Defendant's estimation, at least ten months old. Even if the information relied upon by the affiant is considered to be remote, the additional information found in the affidavit, taken as a whole, clearly overcome any staleness issues.

In sum, the affidavit cites evidence (1) that Defendant has internet service at both his

---

[24] Docket No. 33, Exh. A at ¶49; Exh. B at ¶48.

[25] *Froman*, 355 F.3d at 888 (quoting *United States v. Cherna*, 185 F.3d 403, 407 (5th Cir. 1999)).

[26] *Id.*

[27] *Id.*

residence and office utilizing the same internet service provider and email address; (2) the Defendant's credit card bills reflect charges identical, in amount and in name, to charges independently verified to be from a child pornography website; (3) records from an online credit card collection company associated with a child pornography website reflect the same charges by the Defendant, the same address as one confirmed to be that of the Defendant, as well as the alleged password to the child pornography website which was verified through surveillance of the email address that originated said password; and (4) during the course of the residential search, ICE agents obtained new information that justified probable cause for a search warrant for Defendant's medical office. This evidence leads to a reasonable conclusion that probable cause existed for the issuance and execution of both search warrants in this case.

Defendant also desires the Court to draw a distinction between attempted access and actual access and/or possession of child pornography, in that probable cause exists only when there is evidence the suspect has actually accessed or possessed child pornography. However, the Court is persuaded by the language set forth above from *Flanders* that elucidates the idea that specific information that a defendant is in actual possession of child pornography is unnecessary for a finding of probable cause for a warrant to issue. In addition, the facts presented in the affidavit note that the banner page where ICE agents obtained login and subscription information displayed "more than one dozen images of minors engaging in sexual acts with other minors or adults."[28] From this, a reasonable inference can be drawn that, in the very least, when Defendant purchased his subscriptions he viewed and could have potentially downloaded child pornography to his computer because of the images located on the login page, and his computers would possess evidence of the

[28] Docket No. 33, Exh. A at ¶15; Exh. B at ¶14.

illicit material.

Additionally, as evidenced by the expansive and intricate details of Operation Emissary, an investigation of child pornography involves a multitude of websites, companies, and individuals whose common goal is to elude detection. Given the complicated nature of a child pornography investigation, the evidence may take several months or years to accrue, and that evidence may consist of bits and pieces from several camouflaged sources.

It would frustrate the Fourth Amendment's protection against unreasonable searches and seizures to force those tasked with investigating child pornography to hastily charge an individual based upon incomplete and uncorroborated information because of fear that a more complete investigation would consume too much time, rendering some information stale and unable to support a search warrant. In order to further the aim of the Fourth Amendment, it is better that the investigatory body be given a reasonable amount of time so that it may acquire as much corroborated information concerning the suspect and the alleged activity before taking the next step of entering his home or residence. Consequently, the Court refrains from stating that information that is, at most, thirteen months old is stale as a matter of law. To do so would be inconsistent with Fourth Amendment jurisprudence concerning staleness and probable cause to support a search warrant.

Lastly, the Court finds a distinction between the types of cases where staleness is a major issue, such as cases involving drugs and other evanescent evidence, and cases of child pornography. In cases involving drugs and other evidence which can easily disappear, it is of paramount importance that a search warrant be based upon information closely proximate to the application for the warrant to ensure that "there is a fair probability that contraband or evidence of a crime will be

found in a particular place."[29] Drugs are generally acquired with the intent to resell them in a short period of time, and there is, unfortunately, a ready demand that can liquidate the supply. Child pornography, on the other hand, is not subject to easy and quick disposal, and is generally acquired with the intent of keeping it indefinitely. Consequently, the timeliness of information in support of probable cause for a search warrant for a crime relating to drugs and other evanescent items is different than the requisite timeliness of information in a child pornography case. The former must be based upon recent information to create a fair probability that the evidence sought will be found; whereas the latter may be based upon more remote information because the evidence sought is generally maintained for longer periods of time. Because of this distinction, the age of the information relied upon in an affidavit in support of a search warrant for child pornography is less of a factor than in cases involving evanescent evidence.

For these reasons, the Court finds probable cause existed for the issuance of both the residential and medical office search warrants.

Good Faith Exception to the Exclusionary Rule

Assuming there was insufficient probable cause to support the magistrate's issuance of the search warrant for Defendant's residence, the Court is of the opinion that ICE agents acted in objective reasonable good faith reliance upon the Magistrate Judge's determination that probable cause existed.

Evidence will not be suppressed when the person executing the warrant is objectively reasonable in his "reliance on the magistrate's probable-cause determination and on the technical

[29] *Gates*, 462 U.S. at 238-39 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

sufficiency of the warrant."[30] However, the *Leon* good faith exception is inapplicable if the "affiant's deliberate or reckless material misstatement" causes a warrant to issue.[31] The party opposing "the warrant bears the burden of establishing by a preponderance of the evidence that the misrepresentation was made intentionally or with reckless disregard for the truth."[32]

Here, Defendant makes the argument that ICE agents did not act in good faith in their execution of the search warrant in that (1) the government, in its server searches, failed to uncover an IP address or log files linking Defendant to any illegal website; (2) the government failed to produce evidence showing the Dykstra Email Address, which sent out the passwords and login information, sent an email to Defendant; (3) no evidence was produced proving the illegal child pornography website was operating on the dates Defendant allegedly purchased his subscriptions; and (4) other information the government relied upon was more than four years old and stale.[33]

Defendant fails to cite the specific evidence supporting his assertions that the government failed to act in good faith when it executed the search warrants. The only reference is to Agent DaPaola's testimony, but Defendant fails to cite or provide copies of this testimony. To this end, it appears Defendant has failed its burden of proof. Regardless of the burden of proof issue, the Court is of the opinion that the ample evidence offered by the United States concerning the corroboration of Defendant's name, email address, credit card billing, physical address, and other contact information is sufficient to create a reasonable belief in relying upon the Magistrate Judge's

---

[30] *United States v. Leon*, 468 U.S. 897, 922 (1984).

[31] *United States v. Alvarez*, 127 F.3d 372, 373 (5th Cir. 1997) (citing *Leon*, 468 U.S. at 923).

[32] *Id.*

[33] Docket No. 43 at 5-6.

probable cause determination.

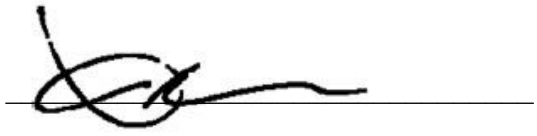
Conclusion

Given both the structure of the child pornography market, and the nature of pornographic material involving children, the information relied upon in the instant case was not stale and was sufficient to provide probable cause to search Defendant's residence and office. A reasonable inference can be drawn that one who purchases a subscription to a child pornography website will take advantage of the access the subscription affords him. Further, it can be reasonably inferred that one suspected of viewing child pornography will maintain an archive of his illicit material. Also, a strict requirement that investigators of suspected child pornography infractions be completed within a shortened period of time would frustrate the protections of the Fourth Amendment. Lastly, child pornography is not the type of evanescent evidence that is susceptible to being disposed of within a short period of time, so timeliness of information in support of a search warrant is a lesser factor in the Court's probable cause analysis than in other cases. Further, the ICE agents relied in good faith on the Magistrate Judge's probable cause determination.

The Court rules that Defendant's Motion to Suppress (Docket No. 29) is **DENIED**.

It is so ORDERED.

SIGNED this 28th day of March, 2008.



XAVIER RODRIGUEZ
UNITED STATES DISTRICT JUDGE